UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/647,644	08/25/2003	Mark Eric Obrecht	6002-00602	2528

7590 09/07/2006

B. Noel Kivlin
Meyertons, Hood, Kivlin, Kowert & Goetzel, P.C.
P.O. Box 398
Austin, TX 78767-0398

EXAMINER	
SHERKAT, AREZOO	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 09/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/647,644	**Applicant(s)** OBRECHT ET AL.	
	Examiner Arezoo Sherkat	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 June 2006*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-104* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-104* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 August 2003* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *6/26/06*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

Response to Amendment

This office action is responsive to Applicant's amendment received on 6/26/2006. Claims 1-104 are pending.

Response to Arguments

Applicant's arguments with respect to claims 1-104 have been considered but are moot in view of the new ground(s) of rejection.

Double Patenting

Claims 1-6, 13-14, 21-34, 41-42, 49-62, 69-70, 77-88, and 95-98 of this application conflict with claims 1-53 of Application No. 10/231,557. 37 CFR 1.78(b) provides that when two or more applications filed by the same applicant contain conflicting claims, elimination of such claims from all but one application may be required in the absence of good and sufficient reason for their retention during pendency in more than one application. Applicant is required to either cancel the conflicting claims from all but one application or maintain a clear line of demarcation between the applications. See MPEP § 822.

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir.

1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 1-6, 13-14, 21-34, 41-42, 49-62, 69-70, 77-88, and 95-98 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-53 of copending Application No. 10/231,557. Although the conflicting claims are not identical, they are not patentably distinct from each other because the language of the claimed limitations are substantially the same and the instant application's claims are the broader version of claims in the copending application No. 10/231,557 (Note: Please refer to the language of claims).

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

Claims 1-5, 13, 21-33, 41, 49-61, 69, 77-87, and 95-97are rejected under 35 U.S.C. 102(e) as being anticipated by Muttik, (U.S. Patent No. 6,775,780).

Regarding claims 1-5, 13, 21-22, 24-25, 41, 49-50, 52-53 and 95-97, Muttik discloses a method for detecting malicious code in an information handling system, comprising:

executing malicious code detection code (MCDC) on the information handling system, the MCDC including detection routines for gathering information about executable code under investigation, the detection routines including at least one of the following: (a) examining the code or program (col. 4, lines 30-45) and (b) searching for information in the information handling system about the code or program (i.e., searching and looking into the database to determine if the actions performed by the code is characteristic of a malicious code profile)(col. 4, lines 1-11), the detection routines including valid program detection routines and malicious code detection routines (i.e., MCDC is the emulator system which detects the malicious code)(col. 3, lines 49-65);

applying the detection routines to the executable code under investigation, the detection routines associating weights to respective code under investigation in response to detections of a valid program or malicious code as a function of at least one of the detection routines, and determining whether code under investigation is a valid program or malicious code as a function of the weights associated by the detection routines, wherein determining whether the code under investigation is a valid program or malicious code includes scoring an execution of the detection routines as a function of the weights (i.e., the detection routines are applied to a given code to associate weights to the code in response to detection of a valid or malicious piece of code)(fig. 2, item 212 – col. 5, lines 14-36).

Regarding claims 69, 77-78, and 80-81, Muttik discloses an information handling system, comprising: a memory, a processor, and a computer-readable code stored by the memory and processable by the processor for detecting malicious code, the computer-readable code including instructions for causing the processor to (col. 3, lines 54-67 and col. 4, lines 1-25):

execute malicious code detection code (MCDC) on the information handling system, the MCDC including detection routines for gathering information about executable code under investigation, the detection routines including at least one of the following: (a) examining the code or program (col. 4, lines 30-45) and (b) searching for information in the information handling system about the code or program (i.e., searching and looking into the database to determine if the actions performed by the code is characteristic of a malicious code profile)(col. 4, lines 1-11), the detection routines including valid program detection routines and malicious code detection routines (i.e., MCDC is the emulator system which detects the malicious code)(col. 3, lines 49-65);

apply the detection routines to the executable code under investigation, the detection routines associating weights to respective code under investigation in response to detections of a valid program or malicious code as a function of at least one of the detection routines, and determine whether code under investigation is a valid program or malicious code as a function of the weights associated by the detection routines, wherein determining whether the code under investigation is a valid program or malicious code includes scoring an execution of the detection routines as a function of the weights (i.e., the detection routines are applied to a given code to associate weights to the code in response to detection of a valid or malicious piece of code)(fig. 2, item 212 – col. 5, lines 14-36).

Regarding claims 23, 51, 79, and 82-83, Muttik discloses wherein the valid program detection routines determine whether the executable code under investigation exhibits at least one or more characteristics and behaviors associated with a valid program, and wherein the malicious code detection routines determine whether the executable code under investigation exhibits at least one or more characteristics and behaviors associated with malicious code (i.e., during the comparison process, the system determines whether or not the record of system calls indicates that code is likely to exhibit malicious behavior)(col. 4, lines 25-56).

Regarding claims 26-27, 54-55, and 80-83, Muttik discloses wherein the scoring algorithm determines a valid program by a summation of weights of the valid program detection routines being greater than a valid program weight threshold, and a malicious code by a summation of weights of the malicious code detection routine having a summed value greater than a malicious code weight threshold (i.e., the system can keep a count of a total weight which is compared against the threshold value)(col. 5, lines 4-36).

Regarding claims 28-31, 56-59, and 84-85, Muttik discloses wherein the detection routines access information about the executable code under investigation from an operating system of the information handling system via Application Programming Interfaces (APIs), and the detection routines gather information from executable code or a program by examining a binary image of the executable code or program, the characteristics and behavior of the executable code or program, and any other related code or programs used by the executable code under investigation (i.e., before executing code, it is analyzed by examining a pattern of system calls (API calls) generated by the code in order to detect potentially malicious behavior)(col. 3, lines 43-67 and col. 4, lines 1-25).

Regarding claims 32, 60, and 86, Muttik discloses delivering malicious code detection code (MCDC) containing the detection routines to the information handling system in a small compact code module via at least one of the following: a computer network, Internet, intranet, extranet, modem line, and prepackaged computer readable storage media (col. 3, lines 10-21).

Regarding claims 33, 61, and 87, Muttik discloses wherein the characteristics and behaviors include at least one of the following: logging keystrokes, saving a display screen view, uploading files, downloading files, executing programs, and controlling the display screen (i.e., activities such as 1-modifying the RunOnce registry key, 2-creating a file, possibly a copy of the same code, which is launched every time the computer restarts, and 3-listening to a non-standard port)(col. 4, lines 1-67 and col. 5, lines 1-14).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 6-12, 14-20, 34-40, 42-48, 62-68, 70-76, 88-94, and 98-104 are rejected under 35 U.S.C. 103(a) as being unpatentable Muttik, (U.S. Patent No. 6,775,780), in view of Chess et al., (U.S. Patent No. 6,560,632 and Chess hereinafter).

Regarding claims 6-12, 14-20, 34-40, 42-48, 62-68, 70-76, 88-94, and 98-104, Muttik discloses wherein the malicious code is code or software program that can compromise security by stealing password, by creating a "back door" into the computer system, or by accessing sensitive information (col. 1, lines 15-25).

Muttik fails to expressly disclose an embodiment wherein the code under investigation may include a Virus, Worm, or a Trojan horse.

However, Chess discloses that Viruses, Worms, and Trojan horses are types of malicious codes (col. 1, lines 65-67 and col. 2, lines 1-28).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Muttik with teachings of Chess because it would allow to include detecting Viruses, Worms, and Trojan horses as types of malicious codes as disclosed by Chess. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Chess to detect malicious code from non-malicious code (Chess, col. 5, lines 20-35).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Arezoo Sherkat whose telephone number is (571) 272-3796. The examiner can normally be reached on 8:00-4:30 Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

A.S.
A. Shurlat
Patent Examiner
Group 2131
August 28, 2006

8/30/2006